

FORM PTO-1449 U.S. Department of Commerce  
(Rev. 4/92) Patent and Trademark Office

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use several sheets if necessary)

ATTY. DOCKET NO.

500.41092X00

SERIAL NO.

10/046,224

APPLICANT

M. NISHIOKA, et al

FILING DATE

January 16, 2002

GROUP

Not assigned

**U.S. PATENT DOCUMENTS**

DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

**FOREIGN PATENT DOCUMENTS**

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT
					YES NO

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

<i>Doc</i>	V.S. Miller, "Use of Elliptic Curves in Cryptography", Proc. Of Crypto' 85, LNCS218, Springer-Verlag, pp. 417-426 (1985).
<i>Doc</i>	S. Goldwasser et al "Probabilistic Encryption, JCSS, 28, 2, pp. 270-299 (1984).
<i>Doc</i>	M. Blum et al, "An Efficient Probabilistic Public-Key Encryption Scheme which hides all partial Information", Proc. Of Crypto '84, LNCS196, Springer-Verlag, pp. 289-299 (1985).

EXAMINER

*David K. ...*

DATE CONSIDERED

5/6/2005

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449 U.S. Department of Commerce  
(Rev. 4/92) Patent and Trademark Office

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use several sheets if necessary)

ATTY. DOCKET NO.

500.41092X00

SERIAL NO.

10/046,224

APPLICANT

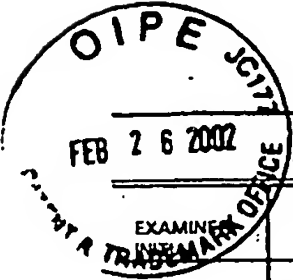
M. NISHIOKA, et al

FILING DATE

January 16, 2002

GROUP

Not assigned



**U.S. PATENT DOCUMENTS**

EXAMINER	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

**FOREIGN PATENT DOCUMENTS**

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT
					YES NO

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

	S. Goldwasser et al, "Lecture Notes on Cryptography", <a href="http://www-cse.ucsd.edu/users/mihir/(1997)">http://www-cse.ucsd.edu/users/mihir/(1997)</a> .
	T. Okamoto et al "A New Public-key Cryptosystem as Secure as Factoring, Proc. Of Eurocrypt '98, LNCS1403, Springer Verlag, pp. 308-318, (1998).
	M. Bellare et al, "Optimal Asymmetric Encryption How to Encrypt with RSA, Proc., of Eurocrypt '94, LNCS950, Springer Verlag, pp. 92-111 (1994).

EXAMINER

DATE CONSIDERED

5/6/2005

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449 U.S. Department of Commerce  
(Rev. 4/92) Patent and Trademark Office

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use several sheets if necessary)

ATTY. DOCKET NO.

500.41092X00

SERIAL NO.

10/046,224

APPLICANT

M. NISHIOKA, et al

FILING DATE

January 16, 2002

GROUP

Not assigned

FEB 26 2002

**U.S. PATENT DOCUMENTS**

EXAMINER	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

**FOREIGN PATENT DOCUMENTS**

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT
					YES NO

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

<i>Doc</i>	R. Cramer et al "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack, Proc. Of Crypto '98, LNCS1462, Springer-Verlag, pp. 13-25, (1998).
<i>Doc</i>	M. Bellare et al "Relations Among Notions of Security for Public-key Encryption Schemes, Proc. Of Crypto '98, LNCS1462, Springer Verlag, pp. 26-45 (1998).

EXAMINER

*David K. Lee*

DATE CONSIDERED

*5/6/2005*

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.